If you are a Linux user for your most of the research work and you come upon the task of debugging Windows kernel, but don't want to switch to a Windows platform for that, QEMU can help you. We can create a virtual serial connection between two QEMU VM. One VM acts as the debugger and the other as debugee, and the virtual connection between them act as the communication channel.

In this tutorial we'll show the steps of creating a virtual serial connection between two QEMU VM.

Prepare Debugee:

First we've to enable debug mode in the debugee (Windows VM to debug). So we run the debugee first. If you are using Windows Vista or later, open a command line in administrator mode and run the following commands:

```
bcdedit /dbgsettings serial debugport:1 baudrate:115200
bcdedit /debug on
```

- Line #1 setup the debug settings
- Line #2 enable the debug mode

If you are using Windows XP [deprecated now], add the following line at the end of your ***C:/boot.ini*** file.

```
multi(0)disk(0)rdisk(0)partition(1)WINDOWS="Windows XP[Debug]"
/fastdetect /debug /debugport=COM1 /baudrate=115200
```

So we are done with setting up the debugee Windows machine in debug mode. We can now shut it down.

Run Debugger:

Use the following QEMU command to start the debugger virtual machine.

```
qemu-system-x86_64 -hda PATH_TO_DEBUGGER_IMAGE_FILE -serial
tcp::1234,server,nowait  -monitor stdio
```

This command will run QEMU and start a TCP server at port 1234. Now when the VM starts up, open WinDbg and configure it for kernel debugging. You just have to set up some parameters in the "Kernel Debugging" popup as following image. You can open the popup

using **CTRL+K** command.


WinDbg Kernel Debugging

Run Debugee and Connect to Debugger:

Next, we'll have to run the debugee. We'll run it using QEMU so that it'll connect to the TCP server created by our previous command. The command to run it:

```
qemu-system-x86_64 -hda PATH_TO_DEBUGEE_IMAGE_FILE   -serial
tcp:localhost:1234 -monitor stdio
```

If everything goes well, the debugee will be connected to the debugger and you'll be able to use WinDbg interface debug.